

## Recipe 19 - Configuration Guide for Setting up RSA Federated Identity Manager 2.5LA as an AA and CS

### Table of Contents:

1	Setup.....	1
1.1	Terms and Introduction .....	1
2	Partner Configuration .....	2
2.1	RSA ClearTrust System Configuration.....	2
2.2	RSA Federated Identity Manager System Configuration.....	5
2.3	Configure a Partner AA.....	24
2.4	Configure a Partner CS .....	29

Version 2.0.0

## 1 Setup

### 1.1 Terms and Introduction

The SAML 1.0 is one of the adopted schemes within the E-Authentication architectural framework. This guide should help you setup SAML 1.0 and RSA Federated Identity Manager v2.5LA as an Agency Application (AA) and Credential Service (CS). Remember that the RSA Federated Identity Manager setup screens are often the same, whether setting up an AA or a CS. After reviewing the terms, configure your scheme to handle SAML 1.0 starting with RSA ClearTrust System Configuration.

Term	Definition
Agency Application (AA)	An online service provided by a government agency that requires an end user to be authenticated.
Credential Service (CS)	A service of a CSP that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential, then each one is considered a separate CS.
Credential Service Provider (CSP)	An organization that offers one or more CSs. Sometimes known as an Electronic Credential Provider (ECP).
Project Management Office (PMO)	The PMO is the organization that handles E-Authentication program management, administration, and operations.

## 2 Partner Configuration

### 2.1 RSA ClearTrust System Configuration

Before configuring RSA Federated Identity Manager as an AA or CS, be sure that the system is properly configured by using RSA ClearTrust. With the administration Graphical User Interface (GUI) servlet container running (generally Tomcat) open a web browser (i.e. Internet Explorer) and go to <http://localhost:8080/adingui/index.jsp>. Login to RSA ClearTrust with administration privileges and follow the instructions provided below.

First, verify that the server has been defined, as well as an application with the appropriate resources. From the RSA ClearTrust home screen, click on **Define Resources > Applications > Manage Existing**, which is demonstrated in Figure 19-1. Applications can be viewed and edited by selecting an application and clicking on **Edit**, which is found in the Edit column of the Applications table. New applications can be added by clicking on the **Add New** button provided above the Applications table.

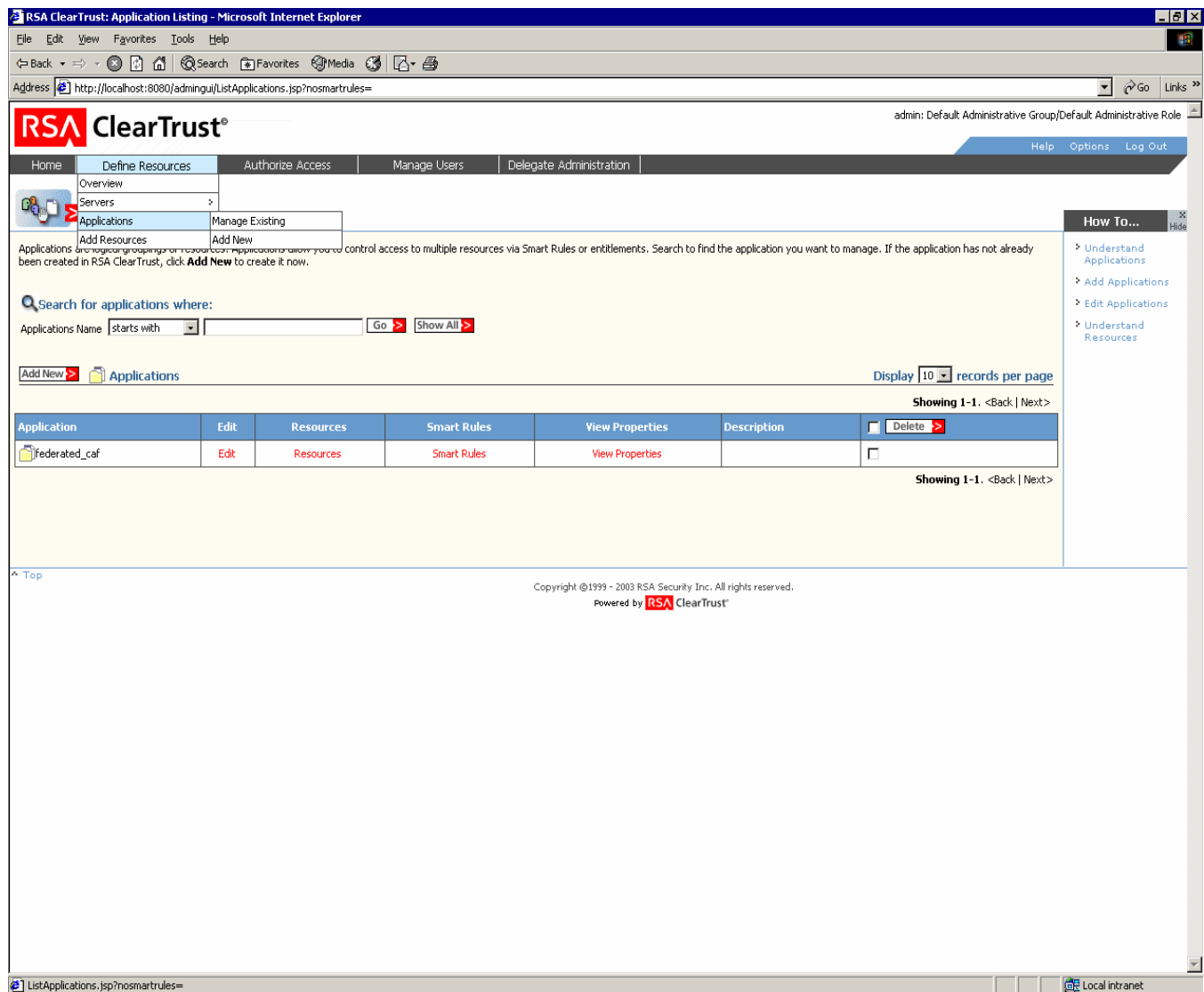


Figure 19-1: Server Verification

Next, verify that users are present and have entitlements to the web application. This is done by clicking on **Manage Users > Users & Administrators**. The Users & Administrators screen will appear as shown in Figure 19-2. Users can be viewed and edited by selecting a user and clicking on **Edit**, which is found in the Edit column of the Users table. New users can be added by clicking on the **Add New** button provided above the Users table.

**RSA ClearTrust®** admin: Default Administrative Group/Default Administrative Role

Home Define Resources Authorize Access **Manage Users** Delegate Administration

**Users & Administrators**

A user is an individual login account in the RSA ClearTrust system. To give this user administrative privileges, select **User is an RSA ClearTrust administrator**.

Search for  where:  starts with   > Advanced Search

Display  records per page

All Showing 1-6. <Back | Next>

User ID	Edit	Entitlements	User Groups	Last Name	First Name	Administrative Group	Delete
admin	Edit	Entitlements	View	Administrator	System	Default Administrative Group	<input checked="" type="checkbox"/>
cbrown	Edit	Entitlements	View	Brown	Chris	Default Administrative Group	<input type="checkbox"/>
tmcbride	Edit	Entitlements	View	Mcbride	Terry	Default Administrative Group	<input type="checkbox"/>
publicj	Edit	Entitlements	View	Q	John	Default Administrative Group	<input type="checkbox"/>
arussell	Edit	Entitlements	View	Russell	Arthur	Default Administrative Group	<input type="checkbox"/>
mtebo	Edit	Entitlements	View	Tebo		Default Administrative Group	<input type="checkbox"/>

Showing 1-6. <Back | Next>

^ Top

Copyright ©1999 - 2003 RSA Security Inc. All rights reserved.  
Powered by **RSA ClearTrust**

**Figure 19-2: Users & Administrators**

After verifying users are present, make sure properties corresponding to the user's attributes you wish to send/receive using SAML assertions have been added. Some properties require modification of the backend user store. This is done by clicking on **Manage Users > Properties**. The Properties screen will appear as shown in Figure 19-3. Properties can be viewed and edited by selecting a property and clicking on **Edit**, which is found in the Edit column of the Properties table. New properties can be added by clicking on the **Add New** button provided above the Properties table.

**RSA ClearTrust®** Properties - Microsoft Internet Explorer

Address: http://localhost:8080/adminui/NavigationProxy.jsp?element=properties

admin: Default Administrative Group/Default Administrative Role

Home Define Resources Authorize Access Manage Users Delegate Administration

Help Options Log Out

Manage Users: Properties

Properties are user attributes that are defined in your database. Once you have defined a property, you can create Smart Rules that allows or deny access to resources based on the value of that property for each user.

Add New > Properties

Display 10 records per page

Showing 1-3. <Back | Next>

Property	Edit	Type	Export	External	Multi-Value	Description	Delete
assuranceLevel	Edit	String	Yes	No	No		<input type="checkbox"/>
commonNameMap	Edit	String	Yes	No	No		<input type="checkbox"/>
csid	Edit	String	Yes	No	Yes		<input type="checkbox"/>

Showing 1-3. <Back | Next>

Copyright ©1999 - 2003 RSA Security Inc. All rights reserved.  
Powered by RSA ClearTrust®

Done Local intranet

**Figure 19-3: Properties**

## 2.2 RSA Federated Identity Manager System Configuration

Next, in RSA Federated Identity Manager, verify attribute plug-ins are present and configured. To access RSA Federated Identity Manager, open a web browser (i.e. Internet Explorer), with the managed server running, go to <http://e1-s3k4.caf.eauth.enspier.net:7001/samlconfig/Index.jsp>, and then log-in with administration privileges.

Plug-ins map users attributes in ClearTrust to the SAML Assertion attributes and vice versa. For E-Authentication participants, plug-ins are available to enable support for required attributes. Please contact RSA for further information regarding plug-ins.

The attribute plug-in for a CS is **RSA SpecialCTAttributePluginAP**, and the attribute plug-in for an AA is **RSA SpecailCTAttributePluginRP**. Attribute plug-ins can be verified by clicking on **Configure System > Plug-Ins > Manage Existing**. The Plug-Ins screen will appear as shown in Figure 19-4. Attribute plug-ins can be viewed and edited by selecting a plug-in and clicking on **Edit**, which is found in the Edit column of the Plug-In table. Attribute plug-ins can be added by clicking on the **Add New** button provided above the Plug-in table.

**RSA Federated Identity Manager**

Home | Asserting Party | Relying Party | Configure System | Help | Log Out

### Plug-Ins

Plug-ins allow you to take advantage of the many SAML mapping and formatting schemes for sending data over the web. You can modify the default plug-ins, or employ RSA Security to write new ones to meet your company's specific needs.

[Add New](#) [Plug-Ins](#)

Plug-In	Edit	Plug-in Type	Description	Delete
RSA_ClearTrust_AP_Attribute_Plug-in	<a href="#">Edit</a>	Attribute	RSA ClearTrust AP Attribute Plug-in	<input type="checkbox"/>
RSA_ClearTrust_RP_Attribute_Plug-in	<a href="#">Edit</a>	Attribute	RSA ClearTrust RP Attribute Plug-in	<input type="checkbox"/>
SpecialCtAttributePluginAP	<a href="#">Edit</a>	Attribute	SpecialCtAttributePluginAP	<input type="checkbox"/>
SpecialCtAttributePluginRP	<a href="#">Edit</a>	Attribute	SpecialCtAttributePluginRP	<input type="checkbox"/>
RSA_ClearTrust_X.509_Subject_Plug-in_AP	<a href="#">Edit</a>	Subject	RSA ClearTrust AP X.509 Subject Plug-in	<input type="checkbox"/>
RSA_ClearTrust_X.509_Subject_Plug-in_RP	<a href="#">Edit</a>	Subject	RSA ClearTrust RP X.509 Subject Plug-in	<input type="checkbox"/>
RSA_FIM_Default_Target_URL_Plug-in	<a href="#">Edit</a>	Target URL	RSA FIM Default Target URL Plug-in	<input type="checkbox"/>
RSA_ClearTrust_Ticket_Plug-in_AP	<a href="#">Edit</a>	Ticket	RSA ClearTrust AP Ticket Plug-in	<input type="checkbox"/>
RSA_ClearTrust_Ticket_Plug-in_RP	<a href="#">Edit</a>	Ticket	RSA ClearTrust RP Ticket Plug-in	<input type="checkbox"/>

[Top](#)

Copyright ©1999 - 2004 RSA Security Inc. All rights reserved.

**Learn About**

- Understanding Plug-Ins
- Managing Plug-Ins

Figure 19-4: View Attribute Plug-Ins

Custom plug-ins are generally java classes that reside in <FIM Home>/rsaappserver/ext. A custom plug-in can be configured as demonstrated in Figure 19-5.

**RSA FIM: Attribute Plug-In - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media Print

Address http://e1-s3k4.caf.eauth.enspiet.net:7001/samlconfig/AttributePlugInAction.do?action=preedit&name=3%2Ccom.rsa.csf.domain.objects.AttributePlugIn Go Links

**RSA Federated Identity Manager** Help Log Out

Home Asserting Party Relying Party Configure System

## Attribute Plug-In

An attribute plug-in defines configuration information to process attributes associated with one or more attribute namespaces.

\* is a required field.

### Attribute Plug-in Basics

☐ Attribute Plug-In Name: \* SpecialCtAttributePluginRP

☐ Class Name: \* com.rsa.csf.techservice.saml.plugins.SpecialCtAttributePluginRP

Description: SpecialCtAttributePluginRP

☐ Created By RSA Security: No

☐ Directory Name: \* specialpluginrp (Do not enter a path)

### Custom Settings

☐ Plug-In Configuration Data:

Name:	Value:

Add

Remove

### Plug-in Class Loading

☐ Action: Load Unload

Cancel Reset Save

^ Top

Copyright ©1999 - 2004 RSA Security Inc. All rights reserved.

Internet

**Figure 19-5: Attribute Plug-In**

Next, from the Plug-Ins screen, verify that subject plug-ins are present and configured. These plug-ins map the local user to the subject of the assertion that is being sent and vice versa.

The subject plug-in for a CS is **RSA\_ClearTrust\_X.509\_Subject\_Plug-in\_AP**, and the subject plug-in for an AAs is **RSA\_ClearTrust\_X.509\_Subject\_Plug-in\_RP**. Subject plug-ins can be viewed and edited by selecting a plug-in and clicking on **Edit**, which is found in the Edit column of the Plug-In table. Subject plug-ins can be added by clicking on the **Add New** button provided above the Plug-In table.

**RSA Federated Identity Manager**

Home | Asserting Party | Relying Party | Configure System | Help | Log Out

## Plug-Ins

Plug-ins allow you to take advantage of the many SAML mapping and formatting schemes for sending data over the web. You can modify the default plug-ins, or employ RSA Security to write new ones to meet your company's specific needs.

[Add New](#) [Plug-Ins](#)

Plug-In	Edit	Plug-in Type	Description	<input type="checkbox"/> Delete
RSA_ClearTrust_AP_Attribute_Plug-in	Edit	Attribute	RSA ClearTrust AP Attribute Plug-in	<input type="checkbox"/>
RSA_ClearTrust_RP_Attribute_Plug-in	Edit	Attribute	RSA ClearTrust RP Attribute Plug-in	<input type="checkbox"/>
SpecialCtAttributePluginAP	Edit	Attribute	SpecialCtAttributePluginAP	<input type="checkbox"/>
SpecialCtAttributePluginRP	Edit	Attribute	SpecialCtAttributePluginRP	<input type="checkbox"/>
RSA_ClearTrust_X.509_Subject_Plug-in_AP	Edit	Subject	RSA ClearTrust AP X.509 Subject Plug-in	<input type="checkbox"/>
RSA_ClearTrust_X.509_Subject_Plug-in_RP	Edit	Subject	RSA ClearTrust RP X.509 Subject Plug-in	<input type="checkbox"/>
RSA_FIM_Default_Target_URL_Plug-in	Edit	Target URL	RSA FIM Default Target URL Plug-in	<input type="checkbox"/>
RSA_ClearTrust_Ticket_Plug-in_AP	Edit	Ticket	RSA ClearTrust AP Ticket Plugin-in	<input type="checkbox"/>
RSA_ClearTrust_Ticket_Plug-in_RP	Edit	Ticket	RSA ClearTrust RP Ticket Plugin-in	<input type="checkbox"/>

Learn About

- Understanding Plug-Ins
- Managing Plug-Ins

Top

Copyright ©1999 - 2004 RSA Security Inc. All rights reserved.

**Figure 19-6: View Subject Plug-Ins**

Figure 19-7 provides an example configuration for a subject plug-in for a CS. The Custom Settings section script maps the user's uid attribute from the LDAP directory to the subject of the assertion.

**RSA FIM: Subject Plug-In - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media Print

Address http://e1-s3k4.caf.eauth.enspiet.net:7001/samlconfig/SubjectMapperPluginAction.do?action=preedit&name=4%2Ccom.rsa.csf.domain.objects.SubjectMapperPlugin Go Links

**RSA Federated Identity Manager** Help Log Out

Home Asserting Party Relying Party Configure System

**Subject Plug-In**

A subject plug-in defines configuration information used to convert between various subject formats, both local and SAML-defined.

\* is a required field.

**Subject Plug-in Basics**

☒ Subject Plug-In Name: \* RSA\_ClearTrust\_X.509\_Subject\_Plug-in\_AP

☒ Class Name: \* com.rsa.csf.techservice.saml.plugins.CTX509SubjectMapperPlugin

Description: RSA ClearTrust AP X.509 Subject Plug-in

☒ Created By RSA Security: Yes

**Supported Subject Formats**

☒ Standard Formats:

- ☒ X.509 Subject Name
- ☐ E-mail Address
- ☐ Windows Domain Qualifier

☒ Custom Formats:

Name: Add Remove

**Custom Settings**

☒ Plug-In Configuration Data:

Name	Value
c:uid:/S09RdnAttribute=uid	c:uid:/S09SubjectTemplate=uid=%CTUID%

Remove

Cancel Reset Save

Done Internet

**Figure 19-7: Subject Plug-In**



Figure 19-8 provides an example configuration for a subject plug-in for an AA. The Custom Settings section script maps the subject of the assertion to the user's uid attribute from the LDAP directory.

**RSA FIM: Subject Plug-In - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Address: <http://e1-s3k4.caf.eauth.enspier.net:7001/samlconfig/SubjectMapperPluginAction.do?action=preedit&name=5%2Ccom.rsa.csf.domain.objects.SubjectMapperPlugin>

**RSA Federated Identity Manager**

Home Asserting Party Relying Party Configure System Help Log Out

## Subject Plug-In

A subject plug-in defines configuration information used to convert between various subject formats, both local and SAML-defined.

\* is a required field.

### Subject Plug-In Basics

**Subject Plug-In Name:** \* RSA\_ClearTrust\_X.509\_Subject\_Plug-in\_RP

**Class Name:** \* com.rsa.csf.techservice.saml.plugins.Ctx509SubjectMapperPlugin

**Description:** RSA ClearTrust RP X.509 Subject Plug-in

**Created By RSA Security:** Yes

### Supported Subject Formats

**Standard Formats:**

- ☒ X.509 Subject Name
- ☐ E-mail Address
- ☐ Windows Domain Qualifier

**Custom Formats:**

Name:  **Add**

**Remove**

### Custom Settings

**Plug-In Configuration Data:**

Name	Value
ctx509SubjectTemplate=uid=%CTUID%	

**Remove**

**Cancel** **Reset** **Save**

Done Internet

**Figure 19-8: Example Subject Plug-In for an AA**

Next, namespaces must be defined. CSs must define an attribute namespace to send in assertions. Currently E-Authentication requires this to be <http://eauthentication.gsa.gov/federated/attribute>. An AA must define subject namespaces that match the namequalifier attribute in the nameidentifier element of assertions received from SAML partners.

Namespaces can be defined by clicking on **Configure System > Namespaces > Manage Existing**. The Namespaces screen should appear as shown in Figure 19-9. Namespaces can be viewed and edited by selecting a namespace and clicking on **Edit**, which is found in the Edit column of the Namespaces table. New namespaces can be added by clicking on the **Add New** button provided above the Namespaces table.

**RSA Federated Identity Manager**

Home | Asserting Party | Relying Party | Configure System | Help | Log Out

## Namespaces

A namespace is a unique identifier that specifies which plug-ins to use to perform specialized processing on subject or attribute data. You reference these namespaces when you configure your trusted relying or asserting parties.

[Add New](#) [Namespaces](#)

Namespace	Edit	Type	Asserting Party Plug-In	Relying Party Plug-In	Description	Delete
<a href="#">http://eauthentication.gsa.gov/federated/attribute</a>	<a href="#">Edit</a>	Attribute	SpecialCtAttributePluginAP	SpecialCtAttributePluginRP		<input type="checkbox"/>
<a href="#">c=us</a>	<a href="#">Edit</a>	Subject	RSA_ClearTrust_X.509_Subject_Plug-in_AP	RSA_ClearTrust_X.509_Subject_Plug-in_RP	IBM	<input type="checkbox"/>
<a href="#">csp.orc.com:443</a>	<a href="#">Edit</a>	Subject	RSA_ClearTrust_X.509_Subject_Plug-in_AP	RSA_ClearTrust_X.509_Subject_Plug-in_RP	ORC	<input type="checkbox"/>
<a href="#">dc=caf,dc=eauth,dc=enspier,dc=net</a>	<a href="#">Edit</a>	Subject	RSA_ClearTrust_X.509_Subject_Plug-in_AP	RSA_ClearTrust_X.509_Subject_Plug-in_RP		<input type="checkbox"/>
<a href="#">e1-s4k1.caf.eauth.enspier.net</a>	<a href="#">Edit</a>	Subject	RSA_ClearTrust_X.509_Subject_Plug-in_AP	RSA_ClearTrust_X.509_Subject_Plug-in_RP		<input type="checkbox"/>
<a href="#">e1-s6k2.caf.eauth.enspier.net</a>	<a href="#">Edit</a>	Subject	RSA_ClearTrust_X.509_Subject_Plug-in_AP	RSA_ClearTrust_X.509_Subject_Plug-in_RP		<input type="checkbox"/>
<a href="#">http://E1-S2K3.caf.eauth.enspier.net</a>	<a href="#">Edit</a>	Subject	RSA_ClearTrust_X.509_Subject_Plug-in_AP	RSA_ClearTrust_X.509_Subject_Plug-in_RP		<input type="checkbox"/>
<a href="#">http://e1-s3k4.caf.eauth.enspier.net</a>	<a href="#">Edit</a>	Subject	RSA_ClearTrust_X.509_Subject_Plug-in_AP	RSA_ClearTrust_X.509_Subject_Plug-in_RP	RSA	<input type="checkbox"/>
<a href="#">http://saml10-16.caf.eauth.enspier.net</a>	<a href="#">Edit</a>	Subject	RSA_ClearTrust_X.509_Subject_Plug-in_AP	RSA_ClearTrust_X.509_Subject_Plug-in_RP		<input type="checkbox"/>
<a href="#">o=u.s. government,c=us</a>	<a href="#">Edit</a>	Subject	RSA_ClearTrust_X.509_Subject_Plug-in_AP	RSA_ClearTrust_X.509_Subject_Plug-in_RP	ORC	<input type="checkbox"/>
<a href="#">saml10-10.caf.eauth.enspier.net</a>	<a href="#">Edit</a>	Subject	RSA_ClearTrust_X.509_Subject_Plug-in_AP	RSA_ClearTrust_X.509_Subject_Plug-in_RP		<input type="checkbox"/>
<a href="#">saml10-13.caf.eauth.enspier.net</a>	<a href="#">Edit</a>	Subject	RSA_ClearTrust_X.509_Subject_Plug-in_AP	RSA_ClearTrust_X.509_Subject_Plug-in_RP		<input type="checkbox"/>
<a href="#">www.netegrity.com</a>	<a href="#">Edit</a>	Subject	RSA_ClearTrust_X.509_Subject_Plug-in_AP	RSA_ClearTrust_X.509_Subject_Plug-in_RP		<input type="checkbox"/>

[Top](#)

Copyright ©1999 - 2004 RSA Security Inc. All rights reserved.

Done Internet

**Learn About**

- Managing Namespaces
- Understanding Namespaces
- Adding an Attribute Namespace
- Adding a Subject Namespace
- Understanding Plug-Ins

**Figure 19-9: Namespaces**

Figure 19-10 provides an example of how to configure an attribute namespace for a CS. Notice this is linked to the subject plug-in provided in the previous step.

**RSA FIM: Attribute Namespace - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media Print

Address <http://e1-s3k4.caf.eauth.enspiet.net:7001/samlconfig/NameSpaceAction.do?action=preedit&name=0,com.rsa.csf.domain.objects.AttributeNSMapper> Go Links

**RSA Federated Identity Manager** Help Log Out

Home Asserting Party Relying Party Configure System

## Attribute Namespace

An attribute namespace is associated with one or more attribute sets. It specifies which data store the attribute names come from and which plug-in to use for processing the attributes at the relying party site.

\* is a required field.

### Attribute Namespace Basics

Attribute Namespace: \*

Description:

### Link to Attribute Plug-In

Asserting Party Plug-In: \*

Relying Party Plug-In: \*

Cancel  Reset  Save

[^ Top](#)

Copyright ©1999 - 2004 RSA Security Inc. All rights reserved.

Done Internet

**Learn About**

- Adding an Attribute Namespace
- Managing Namespaces
- Understanding Namespaces
- Adding an Attribute Plug-In

**Figure 19-10: Attribute Namespace**

For a CS in Asserting Party mode, a namespace corresponding to the value being sent in the namequalifier of the assertion must be created. This is linked to the subject plug-in provided in the previous step. An example of creating a subject namespace is provided in Figure 19-11.

**RSA FIM: Subject Namespace - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media Print

Address <http://e1-s3k4.caf.eauth.ensper.net:7001/samlconfig/SubNameSpaceAction.do?action=preedit&name=7,com.rsa.csf.domain.objects.SubjectNQMapper> Go Links

---

**RSA Federated Identity Manager** Help Log Out

Home Asserting Party Relying Party Configure System

---

**Subject Namespace**

A subject namespace is used in Web SSO assertion statements and SAML queries. It specifies which data store the subject name came from and which plug-in to use for mapping the subject name to a local identity at the asserting party or relying party site.

\* is a required field.

**Subject Namespace Basics**

**Subject Namespace:** \*

**Description:**

**Link to Subject Plug-In**

**Asserting Party Plug-In:** \*

**Relying Party Plug-In:** \*

Cancel  Reset  Save

---

[Top](#)

Copyright ©1999 - 2004 RSA Security Inc. All rights reserved.

Done Internet

**Figure 19-11: Subject Namespace**

For an AA in Relying Party mode, a namespace corresponding to the asserting party's namequalifier from the assertion must be created. An example of creating this namespace is provided in Figure 19-12

**Figure 19-12: Namespace for an AA in Relying Party Mode**

Next, attribute sets need to be configured. This is done by clicking on **Configure System > Attribute Sets**. The Attribute Sets screen should appear as shown in Figure 19-13. For a CS, this is where attribute sets that are sent in the assertion are configured. For an AA, this is where the attribute sets that will be received from SAML partners are configured.

Attribute sets can be viewed and edited by selecting an attribute set and clicking on **Edit**, which is found in the Edit column of the Attribute Sets table. An attribute set can be added by clicking on the **Add New** button provided above the Attribute Sets table.

**RSA FIM: Attribute Sets - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address <http://e1-s3k4.caf.eauth.enspier.net:7001/samlconfig/ListAttributeList.do?action=prelist&domainobject=AttributeList> Go Links

**RSA Federated Identity Manager** Help Log Out

Home Asserting Party Relying Party Configure System

**Attribute Sets**

Attribute sets are named collections of one or more attribute designators that use the same namespace. You reference these attribute sets when you configure your trusted relying or asserting parties.

Add New **Attribute Sets**

Attribute Set Name	Edit	Attribute Namespace	Description	Delete
FOC	Edit	http://eauthentication.gsa.gov/federated/attribute		<input type="checkbox"/>
FOCminusCSID	Edit	http://eauthentication.gsa.gov/federated/attribute		<input type="checkbox"/>
FOCplusgivenName	Edit	http://eauthentication.gsa.gov/federated/attribute		<input type="checkbox"/>

[^ Top](#)

Copyright ©1999 - 2004 RSA Security Inc. All rights reserved.

**Learn About**

- > Managing Attribute Sets
- > Understanding Attribute Sets
- > Adding an Attribute Set
- > Adding an Attribute Namespace

Done Internet

**Figure 19-13: Attribute Sets**

Figure 19-14 provides the properties of an attribute set. The names of the attributes are **assuranceLevel**, **CSid**, and **commonName**. These attributes correspond to user attributes provided in the SAML assertion and the LDAP user store.

**Figure 19-14: Edit Attribute Set**

Next, keystores need to be configured. This is done by clicking on **Configure System > Keystores**. The Keystores screen will appear as shown in Figure 19-15. For a CS (AP mode), this is where a reference to a copy of your SAML partner client SSL certificate is created. For an AA (RP mode), this is where a reference to the client key that will be presented to your SAML provider will be created.

Keystores can be viewed and edited by selecting a namespace and clicking on **Edit**, which is found in the Edit column of the Keystore table. A new keystore can be added by clicking on the **Add New** button provided above the Keystore table.

**RSA Federated Identity Manager**

Home | Asserting Party | Relying Party | **Configure System** | Help | Log Out

## Keystores

Keystores are files containing keys and certificates. They are required to digitally sign requests, responses, or assertions. You reference these keystores when you add your trusted relying or asserting parties.

[Add New](#) [Keystore](#)

Keystore	Edit	Description	Delete
08SAML10-09	<a href="#">Edit</a>		<input type="checkbox"/>
10saml1011	<a href="#">Edit</a>		<input type="checkbox"/>
ORC	<a href="#">Edit</a>	ORC	<input type="checkbox"/>
e1_s2k3_aa	<a href="#">Edit</a>	Entegrity	<input type="checkbox"/>
e1_s3k4	<a href="#">Edit</a>	RSA's Key	<input type="checkbox"/>
e1_s4k1	<a href="#">Edit</a>	HP	<input type="checkbox"/>
e1s6k2_aa	<a href="#">Edit</a>	Entrust II	<input type="checkbox"/>
e1s6k2_cs	<a href="#">Edit</a>	Entrust	<input type="checkbox"/>
e1s7k6_cs	<a href="#">Edit</a>	Entrust III	<input type="checkbox"/>
entegrity_client	<a href="#">Edit</a>		<input type="checkbox"/>
saml10-01	<a href="#">Edit</a>		<input type="checkbox"/>
saml10-10	<a href="#">Edit</a>	ShareID 2.0	<input type="checkbox"/>
saml10-16	<a href="#">Edit</a>	IBM AA	<input type="checkbox"/>
saml1013	<a href="#">Edit</a>	TrustGenix g	<input type="checkbox"/>

[Top](#)

Copyright ©1999 - 2004 RSA Security Inc. All rights reserved.

Done

Internet

**Figure 19-15: Keystores**



For an AA's RSA client key, the **Keystore Path** and **Filename** field is the path to the java keystore where the client key pair is stored. The **Certificate Alias** is the alias in the keystore for the key pair. An AA must supply both the **Keystore Password** and **Private Key Password**. An example of this is provided in Figure 19-16.

**RSA FIM: Edit Keystore - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Address <http://e1-s3k4.caf.eauth.enspier.net:7001/samlconfig/KeyStoreAction.do?action=preedit&pagemode=edit&name=4> Go Links

**RSA Federated Identity Manager** Help Log Out

Home Asserting Party Relying Party Configure System

**Edit Keystore**

Define the configuration information required to access a keystore file on the system. Only keystore files in the Java Key Store (JKS) format are supported. You must import certificates stored in Privacy Encode Mail (PEM) or PKCS #12 (P12) formats into a new or existing JKS file before you can use them.

\* is a required field.

**Keystore Basics**

Keystore Name: \* e1\_s3k4  
 Description: RSA's Key  
 Keystore Path and Filename: \* C:\certs\client\_keystore  
 Certificate Alias: \* mykey

**Passwords**

Keystore Password: \*  
 Confirm Password: \*  
 Private Key Password: \*  
 Confirm Password: \*

Cancel X Reset R Save >

Learn About

- Adding a Keystore
- Understanding Keystores
- Managing Keystores

Top

Copyright ©1999 - 2004 RSA Security Inc. All rights reserved.

Done Internet

**Figure 19-16: Edit Keystore**

For a CS's SAML partner client SSL certificate, the **Keystore Path and Filename** field is the path to the java keystore where the SAML partner's public key is stored. The **Certificate Alias** is the alias in the keystore for the public key. For a CS, the **Keystore Password** must be supplied. An example of this is provided in Figure 19-17.

**RSA FIM: Edit Keystore - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address <http://e1-s3k4.caf.eauth.enspiner.net:7001/samlconfig/KeyStoreAction.do?action=preedit&pagenode=edit&name=5> Go Links

**RSA Federated Identity Manager** Help Log Out

Home Asserting Party Relying Party Configure System

## Edit Keystore

Define the configuration information required to access a keystore file on the system. Only keystore files in the Java Key Store (JKS) format are supported. You must import certificates stored in Privacy Encode Mail (PEM) or PKCS #12 (P12) formats into a new or existing JKS file before you can use them.

\* is a required field.

### Keystore Basics

Keystore Name: \*

Description:

Keystore Path and Filename: \*

Certificate Alias: \*

### Passwords

Keystore Password: \*

Confirm Password: \*

Private Key Password:

Confirm Password:

Cancel  Reset  Save

[Top](#)

Copyright ©1999 - 2004 RSA Security Inc. All rights reserved.

Done Internet

**Learn About**

- Adding a Keystore
- Understanding Keystores
- Managing Keystores

**Figure 19-17: Keystore for a CS SAML Partner Client SSL Certificate**

For a CS (AP mode), in addition to having a copy of the client's certificate, a user in WebLogic, with same name as the subject of the certificate, must be added. This is done by opening a web browser (i.e. Internet Explorer) and going to the WebLogic console (<http://e1-s3k4.caf.eauth.enspier.net:7081/console>). Once the WebLogic Server Console opens, select **csfdomain** > **Security** > **Realms** > **myrealm** > **Users** from the folder menu on the left side of the screen. The myrealm> User screen will appear as shown in Figure 19-18. Next, click on the “Configure a new User” link.

**WebLogic Server Console - Microsoft Internet Explorer**

Address: [http://e1-s3k4.caf.eauth.enspier.net:7081/console/actions/mbean/MBeanFramesetAction?bodyFrameId=wl\\_console\\_frame\\_1106588942945&isNew=false&frameId=wl\\_console\\_frame\\_1106588942946&sideBarFrameId=wl\\_cons...](http://e1-s3k4.caf.eauth.enspier.net:7081/console/actions/mbean/MBeanFramesetAction?bodyFrameId=wl_console_frame_1106588942945&isNew=false&frameId=wl_console_frame_1106588942946&sideBarFrameId=wl_cons...)

**Users**

Connected to: e1-s3k4.caf.eauth.enspier.net:7081 | You are logged in as: system | [Logout](#)

Users are entities that can be authenticated. A user can be a person or software entity, such as a Java client. Each user is given a unique identity within a security realm. BEA recommends assigning users to groups for two reasons: it makes the WebLogic Security Service perform better, and makes it more efficient for administrators who work with large numbers of users.

This Users page displays key information about each user that has been configured in this security realm.

[Configure a new User...](#)

Filter By:  [Filter](#)

User	Description	Provider
<a href="#">system</a>		DefaultAuthenticator
<a href="#">e1-s4k1.caf.eauth.enspier.net</a>	HP	DefaultAuthenticator
<a href="#">08SAML10-10.caf.eauth.enspier.net</a>	FIMM Module user	DefaultAuthenticator
<a href="#">e1-s6k2.caf.eauth.enspier.net</a>	FIMM Module user	DefaultAuthenticator
<a href="#">e1-s2k3.caf.eauth.enspier.net</a>	FIMM Module user	DefaultAuthenticator
<a href="#">csp.orc.com</a>	csp.orc.com	DefaultAuthenticator
<a href="#">08SAML10-09.caf.eauth.enspier.net</a>	IBM	DefaultAuthenticator
<a href="#">saml10-01.caf.eauth.enspier.net</a>	FIMM Module user	DefaultAuthenticator
<a href="#">saml10-13.caf.eauth.enspier.net</a>		DefaultAuthenticator
<a href="#">10saml10-11.caf.eauth.enspier.net</a>	FIMM Module user	DefaultAuthenticator
<a href="#">e1-s7k6.caf.eauth.enspier.net</a>	Entrust	DefaultAuthenticator
<a href="#">saml10-10.caf.eauth.enspier.net</a>	shareid	DefaultAuthenticator
<a href="#">saml10-16.caf.eauth.enspier.net</a>	FIMM Module user	DefaultAuthenticator

Figure 19-18: WebLogic Users

Once you click on the “Configure a New User” link, the myrealm>Create User screen should appear as shown in Figure 19-19. In the **Name** field, add a user whose username is the same as the CN in the Subject DN of the X.509 certificate and then click the **Apply** button.

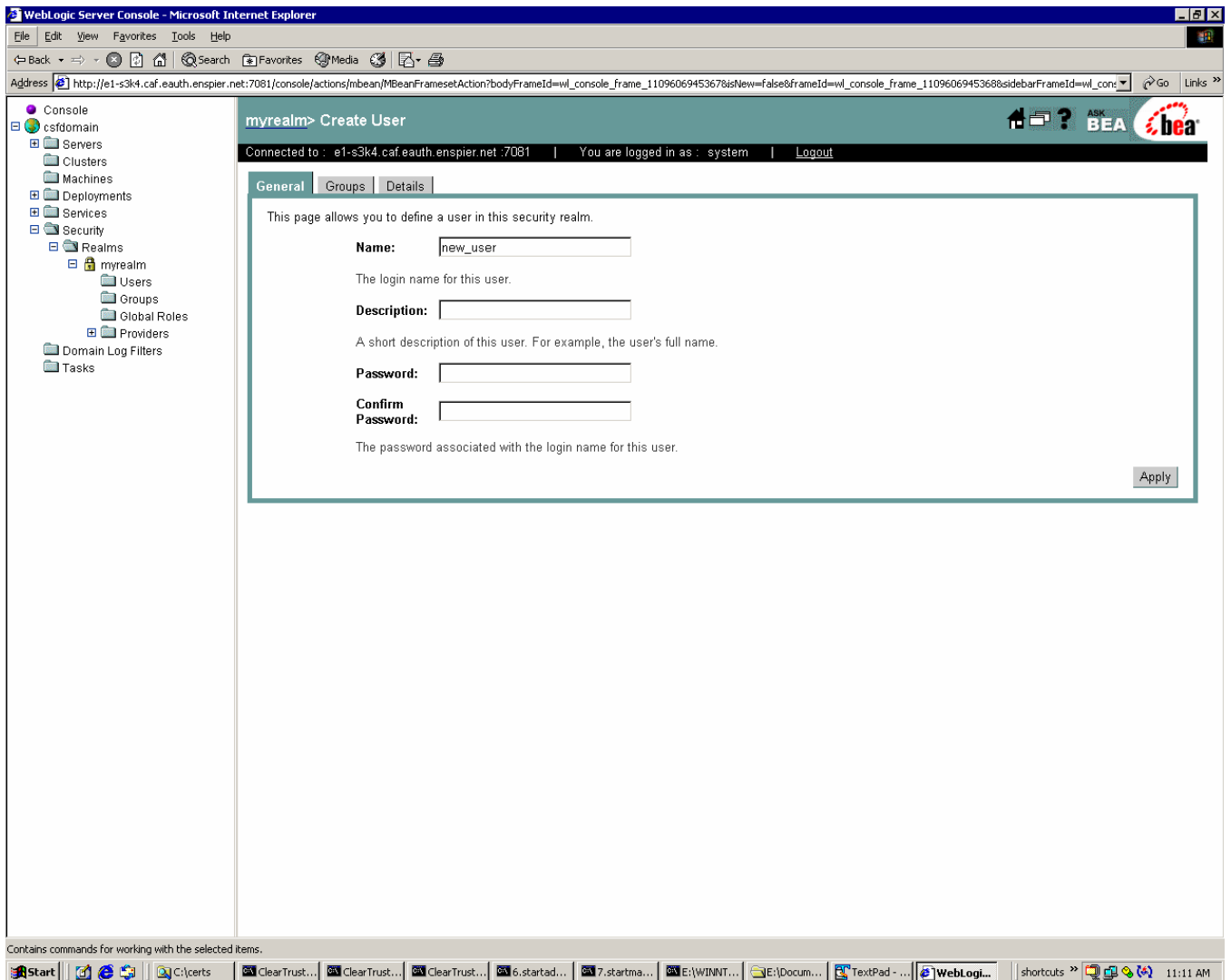
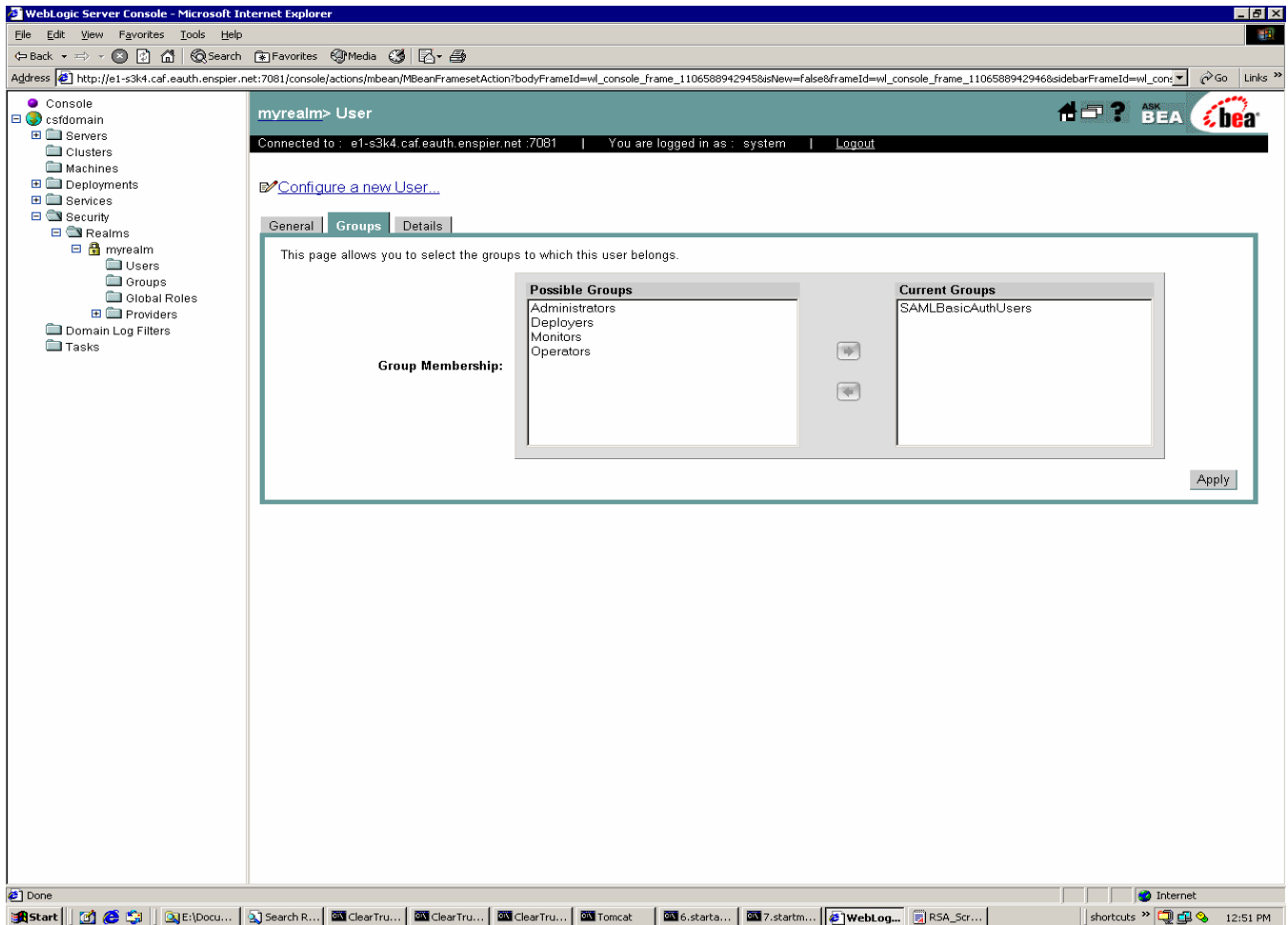


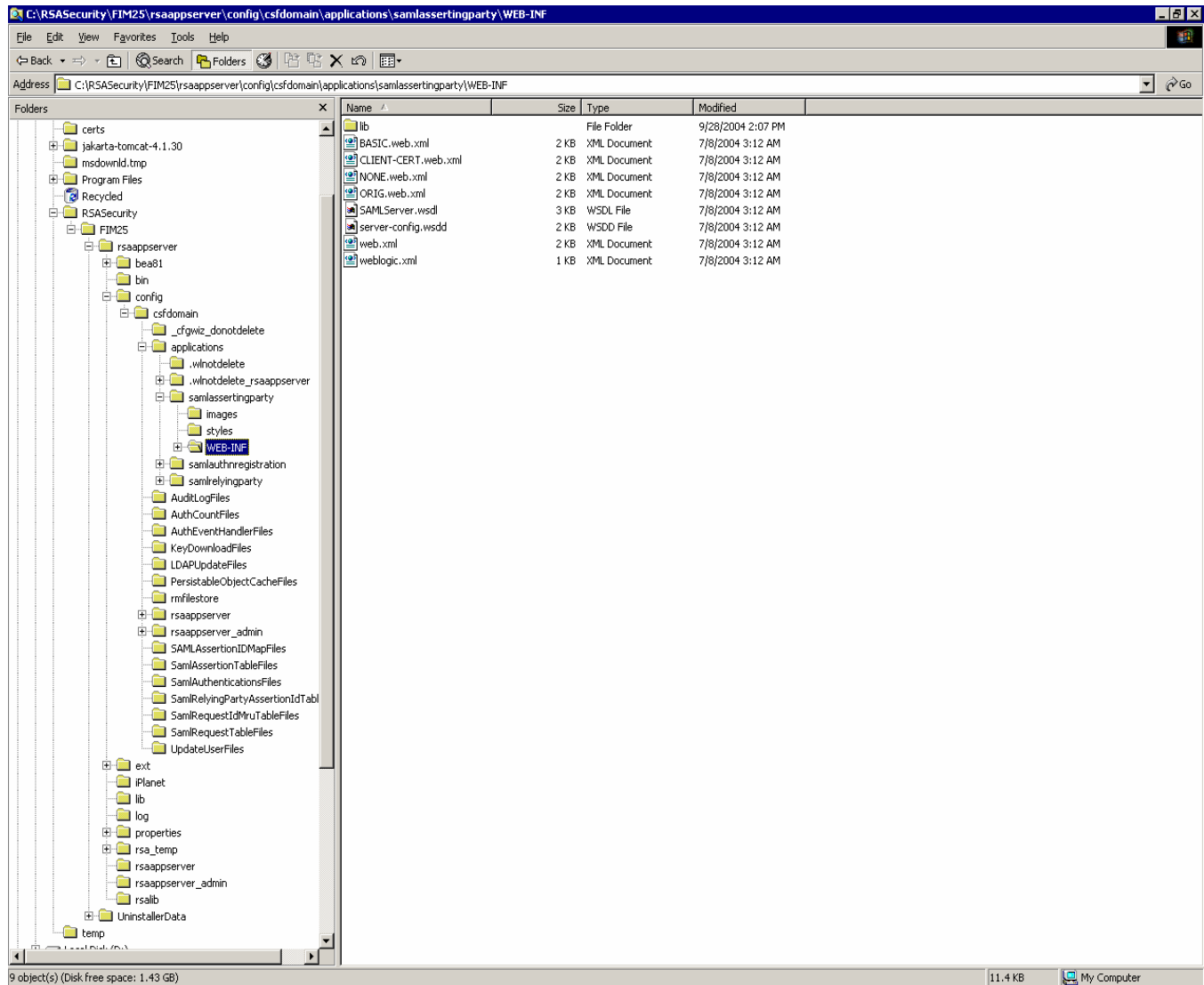
Figure 19-19: myrealm>Create User

Next, add the user created in the previous step to the SAMLBasicAuthUsers group. Click on the **Groups** tab, select the user from the **Possible Groups** column, and click on the → key. This will move the selected user to the **Current Groups** column. To conclude adding the user to the SAMLBasicAuthUsers group, click on the **Apply** button.



**Figure 19-20: Add User to SAMLBasicAuthUsers Group**

Next, verify that the SAMLBasicAuthUsers group is in the web.xml file. The web.xml file can be viewed by opening **Windows Explorer**. From the Windows Explorer folders menu, scroll down until you find **RSASecurity**. Open **RSASecurity > FIM25 > rsaappserver > config > csfdomain > applications > samlAssertingParty > WEB-INF** as demonstrated in Figure 19-21. Once the files stored in the WEB-INF appear, open the **web.xml** file.



**Figure 19-21: Verify SAMLBasicAuthUsers Group**

The text in the web.xml should appear as provided below. Scroll through the text and search for **SAMLBasicAuthUsers**, which should appear as `<role-name>SAML_Basic_Auth_Users</role-name>`.

```
<?xml version="1.0"?>
<!DOCTYPE web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
    "http://java.sun.com/dtd/web-app_2_3.dtd">
<web-app>
    <display-name>SAML Asserting Party</display-name>
    <description>Servlets that provide SAML Asserting Party functionality</description>
    <servlet>
        <servlet-name>SamlSsoAssertingPartyServlet</servlet-name>
        <display-name>SAML SSO Asserting Party Servlet</display-name>
        <description>Servlet that provides SAML SSO Intersite Transfer Service (ISX)
functionality</description>
        <servlet-class>com.rsa.csf.application.saml.SamlSsoAssertingPartyServlet</servlet-class>
    </servlet>
    <servlet>
        <servlet-name>AxisServlet</servlet-name>
        <display-name>Apache-Axis Servlet</display-name>
        <servlet-class>org.apache.axis.transport.http.AxisServlet</servlet-class>
    </servlet>
    <servlet-mapping>
        <servlet-name>SamlSsoAssertingPartyServlet</servlet-name>
        <url-pattern>/AP/*</url-pattern>
    </servlet-mapping>
    <servlet-mapping>
        <servlet-name>AxisServlet</servlet-name>
        <url-pattern>/services/*</url-pattern>
    </servlet-mapping>
    <welcome-file-list>
        <welcome-file>index.html</welcome-file>
    </welcome-file-list>
    <!-- Authentication -->
    <security-constraint>
        <web-resource-collection>
            <web-resource-name>SAML Request</web-resource-name>
            <url-pattern>/services/SamlRequest</url-pattern>
        </web-resource-collection>
        <auth-constraint>
            <role-name>SAML_Basic_Auth_Users</role-name>
        </auth-constraint>
    </security-constraint>
    <login-config>
        <auth-method>CLIENT-CERT</auth-method>
    </login-config>
    <security-role>
        <role-name>SAML_Basic_Auth_Users</role-name>
    </security-role>
</web-app>
```

### 2.3 Configure a Partner AA

From the RSA Federated Identity Manager home screen, click on **Asserting Party > Trusted Relying Parties > Add New**. The Add Trusted Relying Party screen will appear as shown in Figure 19-22. From this screen, select **Specify all the settings yourself** option and select the **Next** button at the bottom of the screen.

Figure 19-22: Add Trusted Relying Party



Next, the Add Trusted Relying Party – Basics screen will appear as shown in Figure 19-23. Enter all the appropriate configuration information as demonstrated below. The **SOAP SSL Keystore** value was predefined in a previous step (Figure 19-15). This is a reference to the SAML partner’s public key which will be presented when requesting an assertion. Once all configuration information has been provided, select the **Next** button at the bottom of the screen.

**RSA FIM: Add Trusted Relying Party - Basics**

Trusted Relying Parties:

## Add Trusted Relying Party - Basics

Basics | Web SSO | Queries | Digital Signatures

**Trusted Relying Party**  
Configure basic SAML settings for this trusted relying party.

\* is a required field.

**Trusted Relying Party Basics**

**Trusted Relying Party Name:** \* Trust Me  
**Description:**

**Identify Via:** Public Key of the SOAP SSL client certificate

**SOAP SSL Keystore:** \* e156k2\_aa

**Recipient URI:** \* http://www.thedomain.com

**Map Local to SAML Authentication Methods**

Local Methods:	maps to	
Basic (Password)	maps to	Password
RSA SecurID	maps to	No Method
Windows NT	maps to	No Method
LDAP	maps to	No Method
Certificate DN	maps to	No Method
Custom	maps to	No Method
Integrated Windows Authentication (IWA)	maps to	No Method

**Audience Restrictions**

**Audience Restriction List:** Restricted URI:  **Add**

**Remove**

**Cancel** **Reset** **Back** **Next**

**Figure 19-23: Add Trusted Relying Party - Basics**

Next, the Add Trusted Relying Party – Web SSO screen will appear as shown in Figure 19-24. Enter all appropriate configuration information as demonstrated below. The Subject Namespace and Attribute Statement refer to what you will send to this partner in your assertion, which were predefined in previous steps (Figure 19-9). Once all configuration information has been provided, select the **Next** button at the bottom of the screen.

**RSA FIM: Add Trusted Relying Party - Web SSO - Microsoft Internet Explorer**

Address: <http://e1-s3k4.caf.eauth.enspier.net:7001/samlconfig/APRPWebSSOAction.do>

**RSA Federated Identity Manager**

Home | Asserting Party | Relying Party | Configure System | Help | Log Out

Trusted Relying Parties: **Add Trusted Relying Party - Web SSO**

Basics | **Web SSO** | Queries | Digital Signatures

**Trusted Relying Party: Trust Me**

Configure Web SSO settings for this trusted relying party.

\* is a required field.

**Web SSO**

☒ Web SSO: ☒ Enable Web SSO

☒ Profile Type:

☒ Artifact Receiver Service URL:   
Example: `https://RP_Server/_Host:7002/samlrelyingparty/RP`

☒ Send Recipient URI: ☐ Send recipient URI in assertions to this Trusted Relying Party

☒ Send Audience Restriction List: ☐ Send audience restriction list in assertions to this Trusted Relying Party

**SAML Subject**

☒ Subject Namespace:

☒ Subject Format:

☒ Send Subject Namespace: ☒ Send subject namespace in assertions to this Trusted Relying Party

☒ Send IP Address: ☐ Send user's browser IP address in assertions to this Trusted Relying Party

☒ Send DNS Address: ☐ Send user's browser DNS address in assertions to this Trusted Relying Party

**Allowed Web SSO Attributes**

☒ Send Attributes: ☒ Send attributes in assertions to this Trusted Relying Party

☒ Attribute Sets: ☒ Available:

Allowed:

javascript:onRSA\_Button('next','APRPWebSSOForm')

**Figure 19-24: Add Trusted Relying Party – Web SSO**

Next, the Add Trusted Relying Party – Queries screen will appear as shown in Figure 19-25. From the Queries section, be sure not to select **Enable attribute and authentication queries** option as demonstrated below. Select the **Next** button at the bottom of the screen.

The screenshot shows a web browser window titled "RSA FIM: Add Trusted Relying Party - Queries - Microsoft Internet Explorer". The address bar shows the URL: <http://e1-s3k4.caf.eauth.enspiet.net:7001/samlconfig/APRPWebSSOAction.do>. The page header includes the RSA logo and "Federated Identity Manager". Navigation tabs include Home, Asserting Party, Relying Party, and Configure System. The main content area is titled "Add Trusted Relying Party - Queries" and features a sub-tabbed interface with "Basics", "Web SSO", "Queries", and "Digital Signatures". The "Queries" tab is active, showing the "Trusted Relying Party: Trust Me" section. Below this, a message states: "Configure attribute and authentication query settings for this trusted relying party. \* is a required field." The "Queries" section contains a checkbox labeled "Enable attribute and authentication queries", which is currently unchecked. At the bottom of the form, there are four buttons: "Cancel", "Reset", "Back", and "Next". The "Next" button is highlighted with a red border. On the right side, a "Learn About" sidebar contains links for "Supported Queries" and "Setting Up Queries". The footer of the page includes a "Top" link and a copyright notice: "Copyright ©1999 - 2004 RSA Security Inc. All rights reserved."

**Figure 19-25: Add Trusted Relying Party – Queries**

Next, the Add Trusted Relying Party – Signatures screen will appear as shown in Figure 19-26. Select all defaults as demonstrated below. Once all defaults have been selected, select the **Save** button at the bottom of the screen. This concludes the configuration of an AA partner.

**RSA Federated Identity Manager**

Home | Asserting Party | Relying Party | Configure System | Help | Log Out

Trusted Relying Parties: **Add Trusted Relying Party - Signatures**

Basics | Web SSO | Queries | **Digital Signatures**

**Trusted Relying Party: testme**

Configure keystores used for signing requests, responses, and assertions. Also, configure settings for certificate and trustlist validation.

\* is a required field.

**Messages Your Domain Receives**

**Requests:** \* Requests from this trusted relying party **Must Not** be signed

**Request Signature Keystore:** \* -- Choose One --

**Messages Your Domain Sends**

**Responses:** ☐ Sign responses sent to this trusted relying party (If BPP, then SAML compliance requires this option.)

**Response Signature Keystore:** \* -- Choose One --

**Assertions:** ☐ Sign assertions sent to this trusted relying party

**Assertion Signature Keystore:** \* -- Choose One --

**Key information:** The verifying certificate will be included with your signed information

**Certificate and Trustlist Verification**

**Verification Method:** Local Verification

Cancel X Reset Back Save

^ Top

Copyright ©1999 - 2004 RSA Security Inc. All rights reserved.

Done Internet

**Figure 19-26: Add Trusted Relying Party - Signatures**

## 2.4 Configure a Partner CS

From the RSA Federated Identity Manager home screen, click on **Relying Party > Trusted Asserting Party > Add New**. The Add Trusted Asserting Party screen will appear as shown in Figure 19-27. Once the screen appears, select **Specify all settings yourself** option and select the **Next** button at the bottom of the screen.

**RSA Federated Identity Manager**

Home | Asserting Party | **Relying Party** | Configure System

Settings and Policies | Trusted Asserting Parties | Manage Existing | **Add New**

### Add Trusted Asserting Party

Depending on your requirements, you may need to specify some or all of the following information to complete the setup of a new trusted asserting party:

- Trusted asserting party name\*
- Issuer ID\*
- SOAP binding service URL, SSL Keystore name, User ID, and password\*
- Source ID
- SAML subject namespace (for Web SSO)\*
- SAML subject format (for Web SSO)
- Basic authentication User ID\*
- Mapping of SAML to local authentication methods
- Attribute sets (for Web SSO)
- Signature keystore names (for digital signing)
- Trustlist verification method
- OCSP Responder URL (for OCSP verification)

Items marked with \* are required for Web SSO Quick Setup. You must set up namespaces, attribute sets, and keystores (if required for your configuration) in Configure System before they are referenced here.

**How do you want to create this new trusted asserting party?**

☐ Web SSO Quick Setup

☒ Specify all settings yourself.

☐ Copy settings from an existing trusted asserting party: -- Choose One --

[Top](#)

Copyright ©1999 - 2004 RSA Security Inc. All rights reserved.

[What You Need Before You Begin](#)

[Choosing a Method](#)

[Using Web SSO Quick Setup](#)

[Specifying All Settings Yourself](#)

[Copying an Existing Trusted Asserting Party](#)

**Figure 19-27: Add Trusted Asserting Party**

Next, the Add Trusted Asserting Party – Basics screen appears as shown in Figure 19-28. Enter all the appropriate configuration information as demonstrated below. Be sure that the **Source ID** is a SHA1 hash of the Issuer ID. In addition, make sure you place the reference of the key pair in the **SOAP SSL Keystore** field. Once all appropriate information has been provided, select the **Next** button at the bottom of the screen.

**RSA FIM: Add Trusted Asserting Party - Basics - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Back Forward Stop Reload Search Favorites Media Print

Address <http://e1-s3k4.caf.eauth.enspier.net:7001/samlconfig/RPAPBasicsAction.do> Go Links

**RSA Federated Identity Manager** Help Log Out

Home Asserting Party Relying Party Configure System

Trusted Asserting Parties: **Add Trusted Asserting Party - Basics**

**Basics** Authentication Web SSO Signatures

**Trusted Asserting Party**

Configure basic SAML settings for this trusted asserting party.

\* is a required field.

**Asserting Party Settings**

**Trusted Asserting Party Name:** \* Test Name

**Description:**

**Issuer ID:** \* <http://www.mydomain.com>

**SOAP Binding Service**

**SOAP Binding Service URL:** \* <http://www.SAMLResponder.com>  
Example: [https://AP\\_Servicelet\\_Host:7002/samlassertingparty/services/SamlRequest](https://AP_Servicelet_Host:7002/samlassertingparty/services/SamlRequest)

**SOAP Connection Type:** SSL Mutual Authentication

**SOAP SSL Keystore:** \* e1\_s3k4

**Source ID**

**Source ID (Base 64):** \* oXob4RfTRT7rjeVF+ACrXXGFp8s= **Generate** **Edit**

**Source ID (Hex):** a17a1be117d3453eeb8de545f800ab5d7185a7cb

Cancel **X** Reset **U** **< Back** **Next >**

Done Internet

**Figure 19-28: Add Trusted Asserting Party - Basics**

Next, the Add Trusted Asserting Party – Authentication screen will appear as shown in Figure 19-29. As demonstrated below, select all the defaults and click on the **Next** button at the bottom of the screen.

**RSA Federated Identity Manager**

Home | Asserting Party | Relying Party | Configure System | Help | Log Out

Trusted Asserting Parties: **Add Trusted Asserting Party - Authentication**

Basics | **Authentication** | Web SSO | Signatures

**Trusted Asserting Party: Test Name**

Specify how every defined and custom SAML authentication method gets translated to a local authentication method. If a SAML method is not used with this asserting party, you must map the SAML method to "No Method".

\* is a required field.

**Map SAML to Local Authentication Methods**

**SAML Method** \* At least one SAML authentication method must be mapped to a local method

Password	maps to	SC_BASIC
Kerberos	maps to	No Method
Secure Remote Password (SRP)	maps to	No Method
Hardware Token	maps to	No Method
SSL/TLS Certificate-Based Client Authentication	maps to	No Method
X.509 Public Key	maps to	No Method
PGP Public Key	maps to	No Method
SPKI Public Key	maps to	No Method
XKMS Public Key	maps to	No Method
XML Digital Signature	maps to	No Method
Unspecified	maps to	No Method

Cancel [X] Reset [R] Back [L] Next [R]

Top

Copyright ©1999 - 2004 RSA Security Inc. All rights reserved.

Done Internet

**Figure 19-29: Add Trusted Asserting Party - Authentication**

Next, the Add Trusted Asserting Party – Web SSO screen will appear as shown in Figure 19-30. Select and enter all appropriate configuration information as demonstrated below. The **Subject Namespace** corresponds to the namequalifier in the assertion that will be received from this partner, and the **Attribute Sets** are those that the sender will include in the assertion. Both of these must be included in the assertion that is received and are predefined under the Configure System options previously described (Figure 19-13). Once all appropriate configuration information has been provided, select the **Next** button at the bottom of the page.

**RSA Federated Identity Manager**

Home | Asserting Party | Relying Party | Configure System | Help | Log Out

Trusted Asserting Parties:

## Add Trusted Asserting Party - Web SSO

Basics | Authentication | **Web SSO** | Signatures

**Trusted Asserting Party: Test Name**

Configure Web SSO settings for this trusted asserting party.

\* is a required field.

**Web SSO**

☒ **Web SSO:** ☒ Enable Web SSO

☒ **Profile Type:**

**SAML Subject**

☒ **Require Subject Namespace:** Assertions  contain a subject namespace

☒ **Subject Namespace:** \*

☒ **Require IP Address:** Assertions  include the browser's IP address

☒ **Require DNS Address:** Assertions  include the browser's DNS address

**Allowed Web SSO Attributes**

☒ **Allow Attribute Statements:** Web SSO assertions  contain an attribute statement

☒ **Attribute Sets:**

Available:		Allowed:
FOCminusCSID	Add >	FOC
FOCplusgivenName		
	Remove <	

Cancel [X] Reset [U] Back [←] Next [→]

**Figure 19-30: Add Trusted Asserting Party – Web SSO**



Next, the Add Trusted Asserting Party – Signatures screen will appear as shown in Figure 19-31. Select all defaults as demonstrated below. Once all defaults have been selected, select the **Save** button at the bottom of the screen. This concludes the configuration of a CS partner.

The screenshot shows the RSA FIM: Add Trusted Asserting Party - Signatures screen in Microsoft Internet Explorer. The browser's address bar shows the URL: <http://e1-s3k4.caf.eauth.enspier.net:7001/samlconfig/RPAPWebSSOAction.do>. The page title is "RSA Federated Identity Manager". The navigation bar includes links for Home, Asserting Party, Relying Party, Configure System, Help, and Log Out. The main content area is titled "Add Trusted Asserting Party - Signatures" and includes a sub-header "Trusted Asserting Party: Test Name". Below this, there is a section for "Messages Your Domain Sends" and "Messages Your Domain Receives". The "Messages Your Domain Sends" section includes fields for "Requests" (with a checkbox for "Sign requests sent to this trusted asserting party"), "Request Signature Keystore" (with a dropdown menu), and "Key information" (with a dropdown menu). The "Messages Your Domain Receives" section includes fields for "Responses" (with a dropdown menu), "Response Signature Keystore" (with a dropdown menu), "Assertions" (with a dropdown menu), and "Assertion Signature Keystore" (with a dropdown menu). Below these sections is a "Certificate and Trustlist Verification" section with a "Verification Method" dropdown menu. At the bottom of the form, there are buttons for "Cancel", "Reset", "Back", and "Save". The page footer includes a "Top" link and a copyright notice: "Copyright ©1999 - 2004 RSA Security Inc. All rights reserved." The browser's status bar at the bottom shows "Done" and "Internet".

Figure 19-31: Add Trusted Asserting Party - Signatures